日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

2

出願年月日
Date of Application: １９９７年 ６月３０日

出願番号
Application Number: 平成 ９年特許願第１７３６７２号

出願人
Applicant (s): 日本電信電話株式会社
エヌティティエレクトロニクス株式会社

PRIORITY DOCUMENT

１９９８年 ７月３１日

特許庁長官
Commissioner,
Patent Office 伴佐山建志

出証番号 出証特平１０－３０６０５１３

【書類名】　特許願

【整理番号】　NTTH095201

【提出日】　平成 9年 6月30日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

【発明の名称】　暗号装置

【請求項の数】　8

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　神田　雅透

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　髙嶋　洋一

【発明者】

【住所又は居所】　東京都武蔵野市吉祥寺本町一丁目１４番５号　エヌ・ティ・ティ・エレクトロニクステクノロジー株式会社内

【氏名】　青木　克彦

【発明者】

【住所又は居所】　神奈川県相模原市上鶴間２６０３－１－２１０

【氏名】　松本　勉

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代表者】　宮津　純一郎

【特許出願人】

【識別番号】　591230295

【氏名又は名称】　エヌ・ティ・ティ・エレクトロニクステクノロジー株式

会社

【代表者】　鈴木　敏正

【代理人】

【識別番号】　100066153

【弁理士】

【氏名又は名称】　草野　卓

【手数料の表示】

【予納台帳番号】　002897

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9701407

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号装置

【特許請求の範囲】

【請求項１】　入力データを初期分割手段で二つの部分データに分割し、これら部分データの一つに対し、非線形関数手段で鍵記憶手段に蓄積された鍵データに依存したデータ変換処理を行い、その非線形関数手段の出力データを前記部分データの他方の一つに線形演算手段で作用させ、その線形演算手段の出力データと前記非線形関数手段の入力部分データとの配列順番を交換手段で交換し、前記交換手段よりこの交換されたデータを二つの部分データとして前記非線形関数手段と、前記線形演算手段と前記交換手段とを繰返し手段で複数回繰返し、前記繰返し手段の最終回の繰返しにおける前記交換手段よりの二つのデータを一つの出力データに最終結合手段で結合して、その出力データを出力する暗号装置において、

前記非線形関数手段は、入力されたデータに前記鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う鍵依存線形変換手段と、

その鍵依存線形手段の出力データを複数個のビット列に分割する分割手段と、

これらビット列にそれぞれ非線形変換を行う第一の非線形変換手段と、

前記第一の非線形変換手段のそれぞれの出力ビット列間で線形変換を行う第一の線形変換手段と、

その第一の線形変換手段の出力ビット列の少くとも一部に非線形変換を行う第二の非線形変換手段と、

その第二の非線形変換手段の出力ビット列を結合して前記非線形関数手段の出力データとする結合手段とを備えることを特徴とする暗号装置。

【請求項２】　請求項１に記載の暗号装置において、

前記結合手段の出力データを線形変換して前記非線形関数手段の出力データとする第二の線形変換手段を備えることを特徴とする暗号装置。

【請求項３】　請求項１または請求項２に記載の暗号装置において、

前記第一の線形変換手段は、前記鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う手段であることを特徴とする暗号装置。

【請求項４】　請求項２に記載の暗号装置において、

前記第二の線形変換手段は、前記鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う手段であることを特徴とする暗号装置。

【請求項５】　請求項１から請求項４までのいずれかに記載の暗号装置において、

前記入力データに線形変換を行って前記初期分割手段へ供給する初期線形変換手段を備えることを特徴とする暗号装置。

【請求項６】　請求項１から請求項５までのいずれかに記載の暗号装置において、

前記最終結合手段の出力データに線形変換を行って暗号装置の出力とする最終線形変換手段を備えることを特徴とする暗号装置。

【請求項７】　請求項５または請求項６に記載の暗号装置において、

前記初期線形変換手段は前記鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う手段であることを特徴とする暗号装置。

【請求項８】　請求項６に記載の暗号装置において、

前記最終線形変換手段は前記鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う手段であることを特徴とする暗号装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、データの通信または蓄積において、データを秘匿するための暗号化装置、特に、秘密鍵の制御のもとでデータをブロック単位で暗号化または復号を行う共通鍵暗号方式による暗号化装置に関するものである。

【０００２】

【従来の技術】

データを秘匿するための暗号化装置に含まれる代表的な共通鍵暗号方式には、米国連邦標準暗号であるＤＥＳ（Data Encryption Standard）暗号がある。

図８は、ＤＥＳ暗号の機能構成を示す。ＤＥＳ暗号では、５６ビットの秘密鍵を用い、６４ビットのデータブロック単位に暗号化または復号を行う。図８にお

いて、暗号化処理は、平文Pの６４ビットを初期変転部１１において初期転値で変換した後、３２ビットごとのブロックデータL_0，R_0に分割される。次に、R_0は図９に示す関数演算部１２への入力として用いられ、関数演算部１２において４８ビットの拡大鍵k_0の制御のもとにｆ（R_0，k_0）に変換される。この変換データｆ（R_0，k_0）とL_0との排他的論理和を回路１３でとり、さらにその値とR_0とを入れ替えて、次のブロックデータL_1，R_1を生成する。すなわち、$R_1 = L_0$（＋）ｆ（R_0，k_0），$L_1 = R_0$である。このように二つのブロックデータL_0，R_0を入力として演算部１２と排他的論理和回路１３とデータの入れ替えとによりL_1，R_1を出力する処理段14_0が構成され、同じような処理段14_1～14_{15}が縦続的に設けられる。つまり各処理段14_i（$0 \leq i < 16$）では、$R_{i+1} = L_i$（＋）ｆ（R_i，k_i），$L_{i+1} = R_i$の処理が行われ、最後にR_{16}，L_{16}を統合して６４ビットにした後、最終転値部１５において最終転値で変換して暗号文６４ビットを出力する。復号処理においては、関数ｆに入力する拡大鍵k_0，k_1，…，k_{14}，k_{15}の順序だけを逆転させて、k_{15}，k_{14}，…，k_1，k_0の順に入力するようにする点を除けば、暗号化処理と同じ手順で実行できる。なお、拡大鍵k_0，k_1，…，k_{14}，k_{15}は、暗号化処理とは別の拡大鍵生成ルーチン１６で５６ビットの秘密鍵が４８ビットの拡大鍵１６個の計７６８ビットに拡大されることによって生成される。

【０００３】

さて、関数演算内部１２の処理は、図９に示すように行われる。まず、３２ビットのブロックデータR_iは拡大転値部１７で４８ビットデータＥ（R_i）に変換される。これに拡大鍵k_iとで排他的論理和を回路１８で取り、４８ビットデータＥ（R_i）（＋）k_iに変換した後、８個の６ビットごとのサブブロックデータに分割する。この８個のサブブロックデータはそれぞれ異なるＳ－ｂｏｘS_0～S_7に入力され、各々が４ビットの出力を得る。なお、このＳ－ｂｏｘS_j（ｊ＝０，１，…，７）は６ビットの入力データから４ビットの出力データに変換する非線形変換テーブルであり、ＤＥＳ暗号の本質的な安全性を担っている部分である。Ｓ－ｂｏｘS_0～S_7の８つの出力データは、再び連結されて３２ビットデータになった後、転置変換部１９を経て、図８に示されるように、L_iと

排他的論理和される関数ｆの出力ｆ（R_i，k_i）となる。

【０００４】

次に、暗号解読法について述べる。ＤＥＳ暗号を始めとする従来の共通鍵暗号方式についてはさまざまな方面から暗号解読が試みられており、そのなかでも、極めて効果的な解読法であるのがE．Biham およびA．Shamirによって提案された差分解読法（“Differential Cryptanalysis of DES-like Cryptosystems．” Proceedings of CRYPTO'90）と松井によって提案された線形解読法（“ＤＥＳ暗号の線形解読法（Ｉ），”１９９３年暗号と情報セキュリティシンポジウムＳＣＩＳ９３－３Ｃ）である。

【０００５】

差分解読法は、２つのデータX，X^* の差分を$\Delta X = X$（＋）X^* としたとき、解読者が入手している平文・暗号文の２組を以下の式に適用して、最終ラウンドにおける拡大鍵k_{15}を求めることを目的としている。

$$f(L_{16}, k_{15})(+) f((L_{16}(+)\ \Delta L_{16}), k_{15}) = \Delta R_{16}(+)\ \Delta R_{14}$$

このとき、L_{16}，ΔL_{16}，ΔR_{16}は暗号文から得られるデータであるので既知の情報である。このため、解読者がΔR_{14}を正しく求めることができるならば、上式はk_{15}のみが未知定数となり、既知の平文・暗号文の組を用いてk_{15}に関する全数探索を行うことで、解読者は必ず正しいk_{15}を見つけだすことができる。一方、ΔR_{14}についてみてみると、この値は中間差分値であるため、一般には求めることが困難である。そこで、１ラウンド目から最終ラウンドの一つ前までのラウンド目までにおいて、各ラウンドが確率p_iで$\Delta R_{i+1} = \Delta L_i$ (+)Δ｛ｆ（ΔR_i）｝，$\Delta L_{i+1} = \Delta R_{i+1}$ のように近似されるとおく。ここでのポイントは、あるΔR_iが入力されたとき、拡大鍵k_iの値に関わらず、確率p_iで Δ｛ｆ（ΔR_i）｝を予測できるということにある。このように近似できるのは、Δ｛ｆ（ΔR_i）｝に影響を与えるのが非線形な変換であるＳ－ｂｏｘの部分だけであり、しかもＳ－ｂｏｘにおいて、入力差分によっては差分出力の分布に極めて大きな偏りが生じるためである。例えば、Ｓ１－ｂｏｘでは、入力差分「１０１００」のとき、１／４の確率で出力差分「００１０」に変換されるためである。そこで、各々のＳ－ｂｏｘが確率p_{si}で入力差分と出力差分との関係が予

測できるとおき、これらを組み合わせることで各ラウンドの近似を求める。さらに、各ラウンドでの近似を連結していくことで、ΔR_{14}は確率$P=\Pi p_i$ でΔL_0，ΔR_0 （ΔL_0，ΔR_0 は平文から得られるデータであるので既知の情報である）から求められることになる。なお、この確率Pが大きいほど、暗号解読が容易である。このようにして、拡大鍵k_{15}が求められると、今度は1段少ない15段ＤＥＳ暗号とみなして、同様の手法で、拡大鍵k_{14}を求めていくということを繰り返して、最終的に拡大鍵k_0 まで求めていく。

【０００６】

Biham らによると、この解読法では、2^{47}組の選択された既知平文・暗号文の組があればＤＥＳ暗号を解読できるとしている。

また、線形解読法は、以下の線形近似式を構成し、解読者が入手している平文・暗号文の組による最尤法を用いて拡大鍵を求めることを目的としている。

$(L_0, R_0)\cdot\Gamma(L_0, R_0)(+)(L_{16}, R_{16})\cdot\Gamma(L_{16}, R_{16}) = (k_0, k_1, \cdots, k_{15})\cdot\Gamma(k_0, k_1, \cdots, k_{15})$

ただし、Γ（Ｘ）はＸの特定のビット位置を選択するベクトルを表し、マスク値という

線形近似式の役割は、暗号アルゴリズム内部を線形表現で近似的に置き換え、平文・暗号文の組に関する部分と拡大鍵に関する部分とに分離することにある。つまり、平文・暗号文の組に関して、平文の特定のビット位置の値と暗号文の特定のビット位置の値との全ての排他的論理和が一定値となり、その値は拡大鍵の特定のビット位置の値の排他的論理和に等しくなることを表している。したがって、解読者は$(L_0, R_0)\cdot\Gamma(L_0, R_0)(+)(L_{16}, R_{16})\cdot\Gamma(L_{16}, R_{16})$の情報から$(k_0, k_1, \cdots, k_{15})\cdot\Gamma(k_0, k_1, \cdots, k_{15})$（１ビット）の情報が得られるということになる。このとき、(L_0, R_0)，(L_{16}, R_{16})はそれぞれ平文・暗号文のデータであるので既知の情報である。このため、解読者が$\Gamma(L_0, R_0)$，$\Gamma(L_{16}, R_{16})$，$\Gamma(k_0, k_1, \cdots, k_{15})$を正しく求めることができるならば、$(k_0, k_1, \cdots, k_{15})\cdot\Gamma(k_0, k_1, \cdots, k_{15})$　（１ビット）を求めることができる。

【０００７】

ＤＥＳ暗号では、非線形な変換が起きる部分はＳ－ｂｏｘしかないため、Ｓ－ｂｏｘについてのみ線形表現ができれば、容易に線形近似式が構成できる。そこで、各々のＳ－ｂｏｘが確率p_{si}で線形表現できるとおく。ここでのポイントは、Ｓ－ｂｏｘに対する入力マスク値が与えられたとき、確率p_{si}でその出力マスク値を予測できるということにある。これは、非線形変換テーブルであるＳ－ｂｏｘにおいて、入力マスク値によっては差分マスク値の分布に極めて大きな偏りが生じるためにおこる。例えば、Ｓ５－ｂｏｘでは、入力マスク値「０１００００」のとき、３／１６の確率で出力マスク値「１１１１」が予測されるためである。これらＳ－ｂｏｘにおけるマスク値を組み合わせることによって、各ラウンドが確率p_iで入力マスク値と出力マスク値のあいだに線形近似することができ、各ラウンドでの線形近似を連結していくことで、$\Gamma(L_0, R_0)$，$\Gamma(L_{16}, R_{16})$，$\Gamma(k_0, k_1, \cdots, k_{15})$は確率$P=2^{n-1}\cdot\Pi|p_i-1/2|$で求められることになる。なお、この確率Ｐが大きいほど、暗号解読が容易である。

【０００８】

松井によると、この解読法で、2^{43}組の既知平文・暗号文の組を用いて、ＤＥＳ暗号の解読に成功している。

さて、上記の解読法に対抗するためには、確率Ｐが十分に小さくなればよい。このため、確率Ｐを小さくするための提案がさまざま行われており、なかでも従来の暗号方式において、もっとも簡単に安全性を高めるための方法がラウンド数を増やすことであった。例えば、ＤＥＳ暗号を３つつなげたTriple-DES暗号は、実質的にＤＥＳのラウンド数を１６段から４８段に増やした暗号方式であり、確率Ｐは、ＤＥＳ暗号よりもはるかに小さい。

【０００９】

【発明が解決しようとする課題】

しかし、上記の解読法に対抗するための対策として、ラウンド数を増加させることは、暗号化速度を犠牲にすることになる。例えば、ラウンド数を３倍に増やせば、暗号化速度は１／３になる。つまり、現在のＤＥＳ暗号の暗号化速度はPentium ＰＣクラスで約１０Ｍｂｐｓであるため、TripleーＤ Ｅ Ｓ暗号ともなると約３．５Ｍｂｐｓまで暗号化速度が低下する。一方で、ネットワークやコンピュ

ータなどは年々高速化しており、暗号化装置もそれらの高速化に対応したものが望まれている。

【0010】

このため、従来の暗号装置では、それらの高速化の要求に対して、安全性と高速性を同時に満たすことはきわめて困難な状況になっている。

この発明の目的は、上記の点を鑑みなされたもので、関数fを安全性と高速性を同時に満たすような構造にすることによって、ラウンド数を増加させることなく安全性を確保し、かつ高速な暗号化処理が可能となるような暗号装置を提供することにある。

【0011】

【課題を解決するための手段】

この発明では、特に非線形関数手段において、非線形関数手段の入力データに鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う鍵依存線形変換手段と、この鍵依存線形変換手段の出力データを複数個のビット列に分割する分割手段と、これら分割された各ビット列に非線形変換をそれぞれ行う第一の非線形変換手段と、その第一の非線形変換手段の各々の出力ビット列間で線形変換を行う第一の線形変換手段と、その第一の線形変換手段の出力ビット列の一部またはすべてに非線形変換を行う第二の非線形変換手段と、その第二の非線形変換手段の出力ビット列をその非線形関数手段の出力データに結合する結合手段とを備えることを特徴とする。

【0012】

さらに安全性を向上させるには、前記結合手段の出力データを前記非線形関数手段の出力データに線形変換を行う第二の線形変換手段を備えることを特徴とする。

また、前記第一の線形変換手段または前記第二の線形変換手段、もしくはその両方の手段が、データの線形変換を行うときに、前記鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う鍵依存線形変換手段であることを特徴とする。

作用

この発明によれば、S－boxにおける確率が$p_{si} \leq p_b < 1$であるとき（p

$_b$はＳ－ｂｏｘの最大確率）、各ラウンドを近似するときの確率は$p_i \leq p_b^{\ 2}$（ただし、差分解読法の場合は関数ｆへの入力差分が０でないとき、線形解読法の場合は関数ｆでの出力マスク値が０でないとき）となることが保証される。また、関数ｆが全単射（入力が異なれば出力が必ず異なる）であるとき、暗号方式のラウンド数を３ｍとすると、暗号方式としての確率は$P \leq p_i^{\ 2m} \leq p_b^{\ 4m}$となる。一般に、暗号方式では$P < 2^{-64}$であれば差分解読法や線形解読法に対して安全とされるため、$m > -16/(\log_2(p_b))$を満たせばよく、$p_b \leq 2^{-4}$であればＤＥＳ暗号の１６ラウンドよりも少ないラウンド数で安全性を確保できる。なお安全性の確率はｍラウンドの倍数ごとに変化する。

【００１３】

また、少なくとも２つのＳ－ｂｏｘが並列に処理できるような配置となっているため、並列処理ができないものと比較して２倍以上の処理速度を出すことが可能である。

ゆえに、差分解読法や線形解読法に対する安全性を、高速な関数で、かつ比較的少ないラウンド数で確保できるため、安全性と高速性を両立させた暗号装置を提供することが可能になる。

【００１４】

【発明の実施の形態】

実施例１

以下、この発明の一実施例を図面を用いて説明する。

図１は、この発明の一実施例を示す暗号装置における、暗号化処理手順の機能構成を示したものである。

【００１５】

平文に相当する入力データＰを入力手段３０１から暗号装置内に入力する。入力データＰは鍵記憶手段３２２に蓄積されている鍵データｆｋによる鍵依存初期線形変換手段３０２で変換された後、初期分割手段３０３で二つのデータL_0，R_0に分割される。例えば６４ビットのデータが３２ビットづつのデータL_0，R_0にビット分割される。データR_0は、鍵記憶手段３２２に蓄積されている鍵データk_{00}，k_{10}，k_{20}とともに非線形関数手段３０４に入力され、非線形関数

手段３０４で変換処理を行われてデータY_0に変換される。データY_0とデータL_0は線形演算手段３０５で演算されてデータ$L_0{}^*$に変換される。データ$L_0{}^*$とデータR_0は交換手段３０６でデータ位置の交換が行われ、$L_1=R_0$，$R_1=L_0{}^*$のように交換される。以下、二つのデータL_1，R_1について上記と同様の処理を繰り返し行う。すなわち、二つのデータL_i，R_iについて、データR_iは、鍵記憶手段３２２に蓄積されている鍵データk_{0i}，k_{1i}，k_{2i}とともに非線形関数手段３０４に入力され、非線形関数手段３０４で変換処理を行われて、データY_iに変換される。データY_iとデータL_iは線形演算手段３０５で演算されてデータ$L_i{}^*$に変換される。データ$L_i{}^*$とデータR_iは交換手段３０６でデータ位置の交換が行われ、$L_{i+1}=R_i$，$R_{i+1}=L_i{}^*$のように交換される。線形演算手段３０５は例えば排他的論理和演算を行うものである。

【００１６】

暗号方式としての安全性を確保するための適切な繰り返し回数をｎとすると、繰り返し処理の結果、データL_n，R_nが得られる。このデータL_n，R_nを最終結合手段３０７で結合しつまり例えば３２ビットの各L_n，R_nをビット結合して６４ビットのデータとし、その後鍵記憶手段３２２に蓄積されている鍵データｅｋによる鍵依存最終線形変換手段３０８で変換し、出力手段３０９から暗号文として出力データＣを出力する。

【００１７】

復号については、暗号化処理手順と逆の手順をたどることによって、暗号文Ｃから平文Ｐが得られる。例えば図１において入力データの代りに暗号文データを入力し、鍵データを図１とは逆に、ｅｋ，$k_{0(n-1)}$，$k_{1(n-1)}$，$k_{2(n-1)}$，…，k_{01}，k_{11}，k_{21}，k_{00}，k_{10}，k_{20}，ｆｋを順次与えればよい。

次に、非線形関数手段３０４の内部を詳細に説明する。図２は、非線形関数手段３０４の内部の機能構成を抜き出して示したものである。

【００１８】

データR_iは、鍵記憶手段３２２に蓄積されている鍵データk_{0i}，k_{1i}，k_{2i}とともに非線形関数手段３０４への入力データとなる。データR_iは、鍵データk_{0i}による鍵依存線形変換手段３４１によりデータ$R_i{}^*$に線形変換される。次

に、データR_i^*は分割手段３４２において例えば８ビットづつの４つのデータin_0，in_1，in_2，in_3にビット分割される。４つのデータin_0，in_1，in_2，in_3は、それぞれ非線形変換手段３４３，３４４，３４５，３４６において、データmid_{00}，mid_{01}，$mid_{02}mid_{03}$に非線形変換された後、鍵依存線形変換手段３４７に入力される。鍵依存線形変換手段３４７では、鍵データk_{1i}により例えば図３に示すように、線形処理される。即ちデータmid_{00}，mid_{01}，mid_{02}，mid_{03}はそれぞれ処理系30_0～30_3に入力され、処理系30_1でmid_{00}とmid_{01}との排他的論理和が回路31_1でとられ、また処理系30_2でmid_{02}とmid_{03}の排他的論理和が回路31_2でとられ、更に回路31_1の出力と回路31_2の出力の排他的論理和が回路32_2でとられる。回路31_1の出力と回路32_2の出力との排他的論理和が回路31_1でとられ、回路33_1の出力とmid_{00}の排他的論理和が回路34_0でとられ、回路32_2の出力とmid_{03}との排他的論理和が回路34_3でとられ、回路34_0，33_1，32_2，34_3の各出力と鍵データk_{1i0},k_{1i1},k_{1i2},k_{1i3}との各排他的論理和が回路35_0～35_3でそれぞれとられて、それぞれmid_{10}，mid_{11}，mid_{12}，mid_{13}を出力する。つまりデータmid_{00}，mid_{01}，mid_{02}，mid_{03}は相互に関連づけられた後、それぞれ鍵データk_{1i0},k_{1i1},k_{1i2},k_{1i3}に依存した線形変換が行われる。論理式で示すと下記の論理演算がなされる。

【００１９】

$mid_{10}= mid_{00}(+)mid_{02}(+)mid_{03}(+)k_{1i0}$,$mid_{11}=mid_{02}(+)mid_{03}(+)k_{1i1}$,

$mid_{12}= mid_{00}(+)mid_{01}(+)mid_{02}(+)mid_{03}(+)k_{1i2}$,$mid_{13}=mid_{00}(+)mid_{01}(+)mid_{02}(+)k_{1i3}$

次にこれらデータmid_{10}，mid_{11}，mid_{12}，mid_{13}は、それぞれ非線形変換手段３４８，３４９，３５０，３５１において、データout_0，out_1，out_2，out_3に非線形変換された後、結合手段３５２において、一つのデータY_i^*に結合される。つまり例えば４つの８ビットのデータが１つの３２ビットデータにビット結合される。最後に、データY_i^*は、鍵データk_{2i}による鍵依存線形変換手段３５３において、データY_iに線形変換され、非線形関

数手段３０４からの出力データY_iが生成される。非線形変換手段３４３～３４６，３４８～３５１の各１つの手段それぞれ、例えばＤＥＳ暗号のＳ－ｂｏｘの１つの要素のようなもので、それぞれ入力データに応じた異った出力データを出力するものである。

【００２０】

ここで、非線形変換手段３４３～３４６は４つ並列に配置されており、その変換処理は相互に関連していないため、これらは並列実行が可能である。また、非線形変換手段３４８～３５１についても同様のことがいえる。

さらに、非線形変換手段３４８～３５１については、鍵依存線形変換手段３４７が任意の鍵依存線形変換方法をとることを可能にするために配置されている。このため、鍵依存線形変換手段３４７が、例えば図３のように特定の線形変換であることがあらかじめわかっている場合には、非線形変換手段３４８～３５１の一部を削除しても、差分解読法および線形解読法に対する安全性が低下しないようにすることができ、削除した分だけ暗号化処理速度の向上が望める。例えば、鍵依存線形変換手段３４７が図３で表されているとき、非線形変換手段３４９，３５０を削除しても差分解読法および線形解読法に対する安全性は低下しない一方で、暗号化速度が約３３％向上する。つまり鍵依存線形変換手段３４７が予め決っている場合は差分解読法、線形解読法に対しては非線形変換手段３４８～３５１の一部はその存在が安全性に関係ない場合があり、その部分は省略できる。

なお、鍵データｆｋ，k_{00}，k_{10}，k_{20}，k_{01}，k_{11}，k_{21}，…，$k_{0(n-1)}$，$k_{1(n-1)}$，$k_{2(n-1)}$，ｅｋは図１において鍵入力手段３２０から暗号装置内に入力された鍵情報Ｋｅｙから鍵データ生成手段３２１によって変換され、鍵記憶手段３２２に蓄積されたデータである。鍵データ生成手段３２１による鍵データの生成はＤＥＳ暗号の拡大鍵生成アルゴリズム１６と同様に行うことができる。

【００２１】

上記のように構成された暗号装置の場合、例えば、非線形変換手段３４３～３４６，３４８～３５１の各１つづつが差分解読法および線形解読法に対して確率$p_b = 2^{-6}$で近似表現できるように設計されているならば、各ラウンドは非線形

変換を必ず２回行うため、確率$p_i \leq 2^{-12}$で近似表現することができ、暗号装置全体としてはラウンド数を３ｍとして、確率$P \leq 2^{-24m}$で近似表現できることになる。ここで、例えばｍ＝４（ラウンド数１２段）とすると、$P \leq 2^{-96}$となり、差分解読法および線形解読法に対して十分安全な暗号装置となる。

【００２２】

また、鍵依存初期線形変換手段３０２、鍵依存最終線形変換手段３０８、鍵依存線形変換手段３４７，３５３は鍵に依存する線形変換手段であるため、差分解読法および線形解読法以外の解読法に対しても十分な安全性を兼ね備え、もっとも安全性を重視した暗号装置である。

なお、この発明はこの例に特定されるだけでなく、例えば高速性を望むのであれば、これら鍵依存初期線形変換手段３０２、鍵依存最終線形変換手段３０８、鍵依存線形変換手段３５３については、そのいずれか、もしくはすべてを削除することが可能である。この場合、差分解読法および線形解読法に対する安全性は低下しない一方で、削除した分だけ暗号化処理速度の向上が望める。ただし他の解読法に対しては弱くなるおそれはある。また、鍵依存初期線形変換手段３０２、鍵依存最終線形変換手段３０８、鍵依存線形変換手段３４７，３５３のいずれか、もしくはすべてを鍵に依存しない線形変換手段に変更することも可能である。この場合、差分解読法および線形解読法以外の解読法に対しても安全性が低下しない一方で、インプリメントを最適化することにより、暗号化処理速度の向上が望める。なお、線形変換手段としては、ビット位置を予め決めた関係で入れかえる転置、予め決めたビット数だけ回転シフトするなどを行う。鍵依存線形変換手段は、鍵データに応じたビット数だけ回転シフトする、あるいは、鍵データとの排他的論理和演算を行うものなどである。

実施例２

図４は、この発明の他の実施例を示す。

【００２３】

平文に相当する入力データＰを入力手段３０１から暗号装置内に入力する。入力データＰは初期分割手段３０３で二つのデータL_0，R_0に分割される。データR_0は、鍵記憶手段３２２に蓄積されている鍵データk_{00}，k_{20}とともに非線

形関数手段３０４に入力され、非線形関数手段３０４で変換処理を行われて、データY_0に変換される。データY_0とデータL_0は線形演算手段３０５で演算され、データ$L_0{}^*$に変換される。データ$L_0{}^*$とデータR_0は交換手段３０６でデータ位置の交換が行われ、$L_1 = R_0$，$R_1 = L_0{}^*$のように交換される。以下、二つのデータL_1，R_1について上記と同様の処理を繰り返し行う。すなわち、二つのデータL_i，R_iについて、データR_iは、鍵記憶手段３２２に蓄積されている鍵データk_{0i}，k_{2i}とともに非線形関数手段３０４に入力され、非線形関数手段３０４で変換処理を行われて、データY_iに変換される。データY_iとデータL_iは線形演算手段３０５で演算され、データ$L_i{}^*$に変換される。データ$L_i{}^*$とデータR_iは交換手段３０６でデータ位置の交換が行われ、$L_{i+1} = R_i$，$R_{i+1} = L_i{}^*$のように変換される。

【００２４】

暗号方式としての安全性を確保するための適切な繰り返し回数をｎとすると、繰り返し処理の結果、データL_n，R_nが得られる。このデータL_n，R_nを最終結合手段３０７で結合した後、出力手段３０９から暗号文として出力データＣを出力する。

復号については、暗号化処理手順と逆の手順をたどることによって、暗号文Ｃから平文Ｐが得られる。

【００２５】

次に、非線形関数手段３０４の内部を詳細に説明する。図５Ａは、非線形関数手段３０４の内部の機能構成を抜き出して示したものである。

データR_iは、鍵記憶手段３２２に蓄積されている鍵データk_{0i}，k_{2i}とともに非線形関数手段３０４への入力データとなる。データR_iは、データk_{0i}による鍵依存線形変換３４１において、データ$R_i{}^*$に線形変換される。次に、データ$R_i{}^*$は分割手段３４２において４つのデータin_0，in_1，in_2，in_3に分割される。４つのデータin_0，in_1，in_2，in_3は、それぞれ非線形変換手段３４３，３４４，３４５，３４６において、データmid_{00}，mid_{01}，mid_{02}，mid_{03}に非線形変換された後、線形変換手段３５４に入力される。線形変換手段３５４では、例えば図５Ｂに示すように相互に関連づけるよ

うに変換される。これは図３中の鍵データとの論理演算を省略した場合と同一の例であり、下記の式で表わせる。

【００２６】

$mid_{10}= mid_{00}(+)mid_{02}(+)mid_{03}, mid_{11}=mid_{02}(+)mid_{03},$

$mid_{12}= mid_{00}(+)mid_{01}(+)mid_{02}(+)mid_{03}, mid_{13}=mid_{00}(+)mid_{01}(+)mid_{02}$

この線形変換で、データmid_{10}，mid_{11}，mid_{12}，mid_{13}が生成され、そのうちのデータmid_{10}，mid_{13}は、それぞれ非線形変換手段３４８，３５１において、データout_0，out_3に非線形変換された後、結合手段３５２において、４つのデータout_0，mid_{11}，mid_{12}，out_3を一つのデータY_i^*に結合される。最後に、データY_i^*は、データk_{2i}による鍵依存線形変換手段３５３において、データY_iに線形変換され、非線形関数手段３０４からの出力データY_iが生成される。

【００２７】

ここで、非線形変換手段３４３～３４６は４つ並列に配置されており、その変換処理は相互に関連していないため、これらは並列実行が可能である。また、非線形変換手段３４８，３５１についても同様のことがいえる。

なお、鍵データk_iは、鍵入力手段３２０から暗号装置内に入力された鍵情報Ｋｅｙから鍵データ生成手段３２１によって変換され、鍵記憶手段３２２に蓄積されたデータである。

【００２８】

上記のように構成された暗号装置の場合、例えば、非線形変換手段３４３～３４６，３４８，３５１が差分解読法および線形解読法に対して確率$p_b = 2^{-6}$で近似表現できるように設計されているならば、実施例１と同様に各ラウンドは確率$p_i \leq 2^{-12}$で近似表現することができ、暗号装置全体としてはラウンド数を３ｍとして、確率$p \leq 2^{-24m}$で近似表現できることになる。ここで、例えばｍ＝４（ラウンド数１２段）とすると、$P \leq 2^{-96}$となり、差分解読法および線形解読法に対して十分安全な暗号装置となる。

【００２９】

また、鍵依存線形変換手段３５３があるため、差分解読法と線形解読法以外の

解読法に対しても安全性にマージンがある構造であり、かつ実施例１よりも構造が簡素化されているため、高速である。つまり、安全性と高速性のバランスを重視した暗号装置である。

実施例３

図６は、この発明の更に他の実施例を示す。

【００３０】

平文に相当する入力データＰを入力手段３０１から暗号装置内に入力する。入力データＰは初期分割手段３０３で二つのデータL_0，R_0に分割される。データR_0は、鍵記憶手段３２２に蓄積されている鍵データk_0とともに非線形関数手段３０４に入力され、非線形関数手段３０４で変換処理を行われて、データY_0に変換される。データY_0とデータL_0は線形演算手段３０５で演算され、データ$L_0{}^*$に変換される。データ$L_0{}^*$とデータR_0は交換手段３０６でデータ位置の交換が行われ、$L_1 = R_0$，$R_1 = L_0{}^*$のように変換される。以下、二つのデータL_1，R_1について上記と同様の処理を繰り返し行う。すなわち、二つのデータL_i，R_iについて、データR_iは、鍵記憶手段３２２に蓄積されている鍵データk_iとともに非線形関数手段３０４に入力され、非線形関数手段３０４で変換処理を行われて、データY_iに変換される。データY_iとデータL_iは線形演算手段３０５で演算され、データ$L_i{}^*$に変換される。データ$L_i{}^*$とデータR_iは交換手段３０６でデータ位置の交換が行われ、$L_{i+1} = R_i$，$R_{i+1} = L_i{}^*$のように変換される。

【００３１】

暗号方式としての安全性を確保するための適切な繰り返し回数をｎとすると、繰り返し処理の結果、データL_n，R_nが得られる。このデータL_n，R_nを最終結合手段３０７で結合した後、出力手段３０９から暗号文として出力データＣを出力する。

復号については、暗号化処理手順と逆の手順をたどることによって、暗号文Ｃから平文Ｐが得られる。

【００３２】

次に、非線形関数手段３０４の内部を詳細に説明する。図７は、非線形関数手

段３０４の機能構成を抜き出して示したものである。

非線形関数手段３０４への入力データR_iは、鍵記憶手段３２２に蓄積されている鍵データk_iとともに鍵依存線形変換３４１への入力となる。データR_iは、データk_iによる鍵依存線形変換３４１において、データR_i^*に線形変換される。次に、データR_i^*は分割手段３４２において４つのデータin_0，in_1，in_2，in_3に分割される。４つのデータin_0，in_1，in_2，in_3は、それぞれ非線形変換手段３４３，３４４，３４５，３４６において、データmid_{00}，mid_{01}，mid_{02}，mid_{03}に非線形変換された後、線形変換手段３５４に入力される。線形変換手段３５４では、例えば実施例２の図５Ｂと同じように、

$mid_{10}= mid_{00}(+)mid_{02}(+)mid_{03}$, $mid_{11}=mid_{02}(+)mid_{03}$,

$mid_{12}= mid_{00}(+)mid_{01}(+)mid_{02}(+)mid_{03}$, $mid_{13}=mid_{00}(+)mid_{01}(+)mid_{02}$

に線形変換し、データmid_{10}，mid_{11}，mid_{12}，mid_{13}を生成する。ついで、データmid_{10}，mid_{13}は、それぞれ非線形変換手段３４８，３５１において、データout_0，out_3に非線形変換された後、結合手段３５２において、４つのデータout_0，mid_{11}，mid_{12}，out_3を一つのデータに結合され、非線形関数手段３０４からの出力データY_iが生成される。

【００３３】

ここで、非線形変換手段３４３～３４６は４つ並列に配置されており、その変換処理は相互に関連していないため、これらは並列実行が可能である。また、非線形変換手段３４８，３５１についても同様のことがいえる。

なお、鍵データk_iは、鍵入力手段３２０から暗号装置内に入力された鍵情報Ｋｅｙから鍵データ生成手段３２１によって変換され、鍵記憶手段３２２に蓄積されたデータである。

【００３４】

上記のように構成された暗号装置の場合、例えば、非線形変換手段３４３～３４６，３４８，３５１が差分解読法および線形解読法に対して確率$p_b = 2^{-6}$で近似表現できるように設計されているならば、各ラウンドは確率$p_i \leq 2^{-12}$で近似表現することができ、暗号装置全体としてはラウンド数を３ｍとして、確率

$P \leq 2^{-24m}$で近似表現できることになる。ここで、例えばm＝4（ラウンド数12段）とすると、$P \leq 2^{-96}$ となり、差分解読法および線形解読法に対して十分安全な暗号装置となる。

【0035】

また、差分解読法および線形解読法に対して十分な安全性を確保するために最低限必要な手段しか実行しない構造であるため、もっとも高速性を重視した暗号装置である。

上述において、非線形関数手段304中の各分割手段342は4分割に限らず、複数に分割すればよい。なお、4分割の場合においては、第二の非線形変換手段は図5A、図7に示したように二つのみとすることができる。

【0036】

【発明の効果】

以上、詳細に説明したように、この発明によれば、非線形関数手段で入力データを複数に分割し、かつそれぞれ非線形変換を行い、その後、相互に線形交換を行い、更に少くとも一部を非線形交換することによりデータの通信または蓄積においてデータを秘匿するための暗号装置について、安全性が高く、かつ高速性を兼ね備えた暗号装置を提供することができる。

【図面の簡単な説明】

【図1】

この発明の実施例1の機能構成を示す図。

【図2】

実施例1における非線形関数手段304の詳細な機能構成例を示す図。

【図3】

図2中の鍵依存線形変換手段347の具体例を示す図。

【図4】

この発明の実施例2の機能構成を示す図。

【図5】

Aは実施例2における非線形関数手段304の詳細な機能構成を示す図、Bはこの手段304中の具体例を示す図である。

【図６】

この発明の実施例３の機能構成を示す図。

【図７】

実施例３における非線形関数手段３０４の詳細な機能構成を示す図。

【図８】

従来のＤＥＳ暗号装置の機能構成を示す図。

【図９】

図８中のｆ関数演算部１２の具体的機能構成を示す図。

【書類名】　図面

【図１】

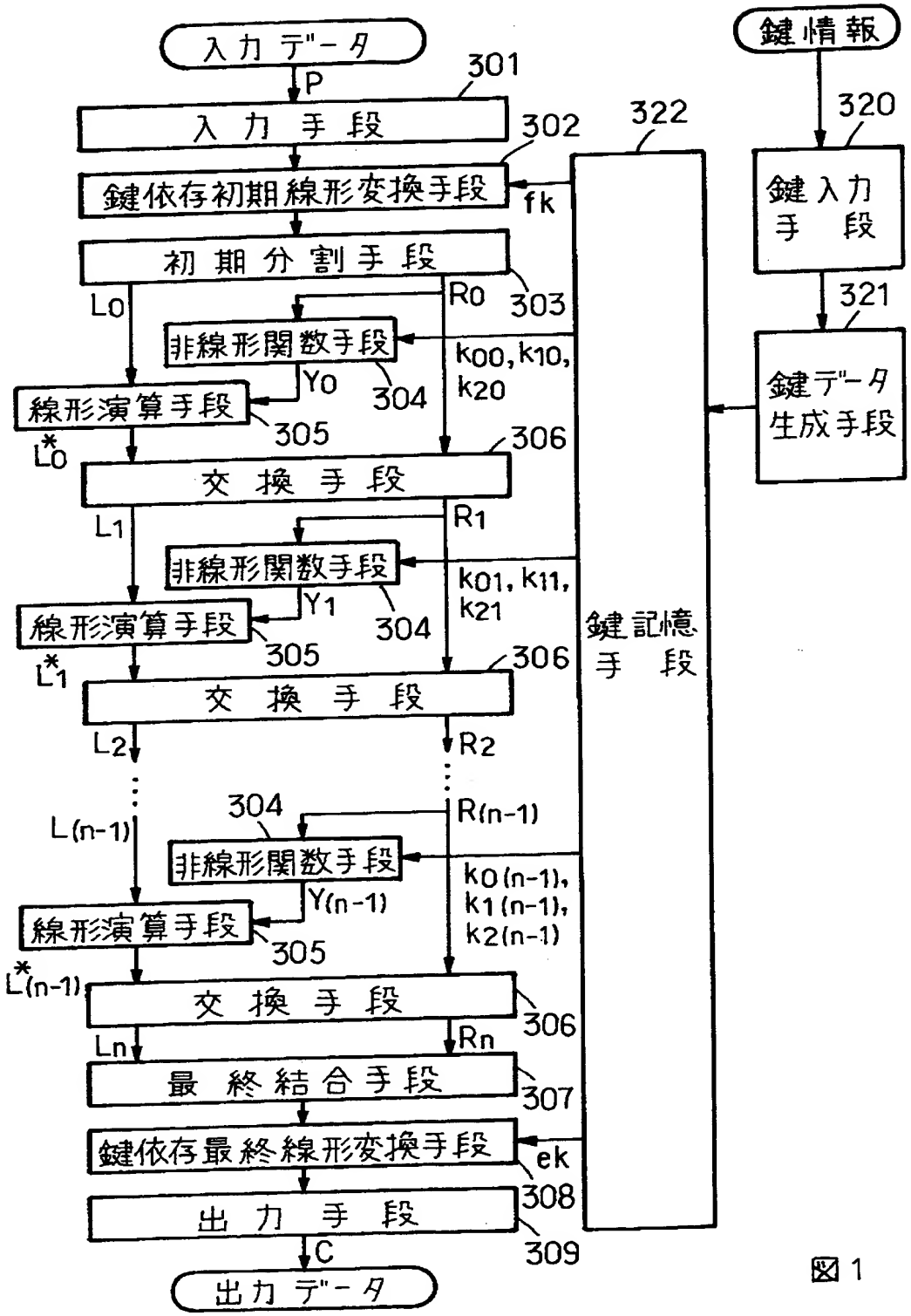

図１

出証特平１０－３０６０５１３

【図２】

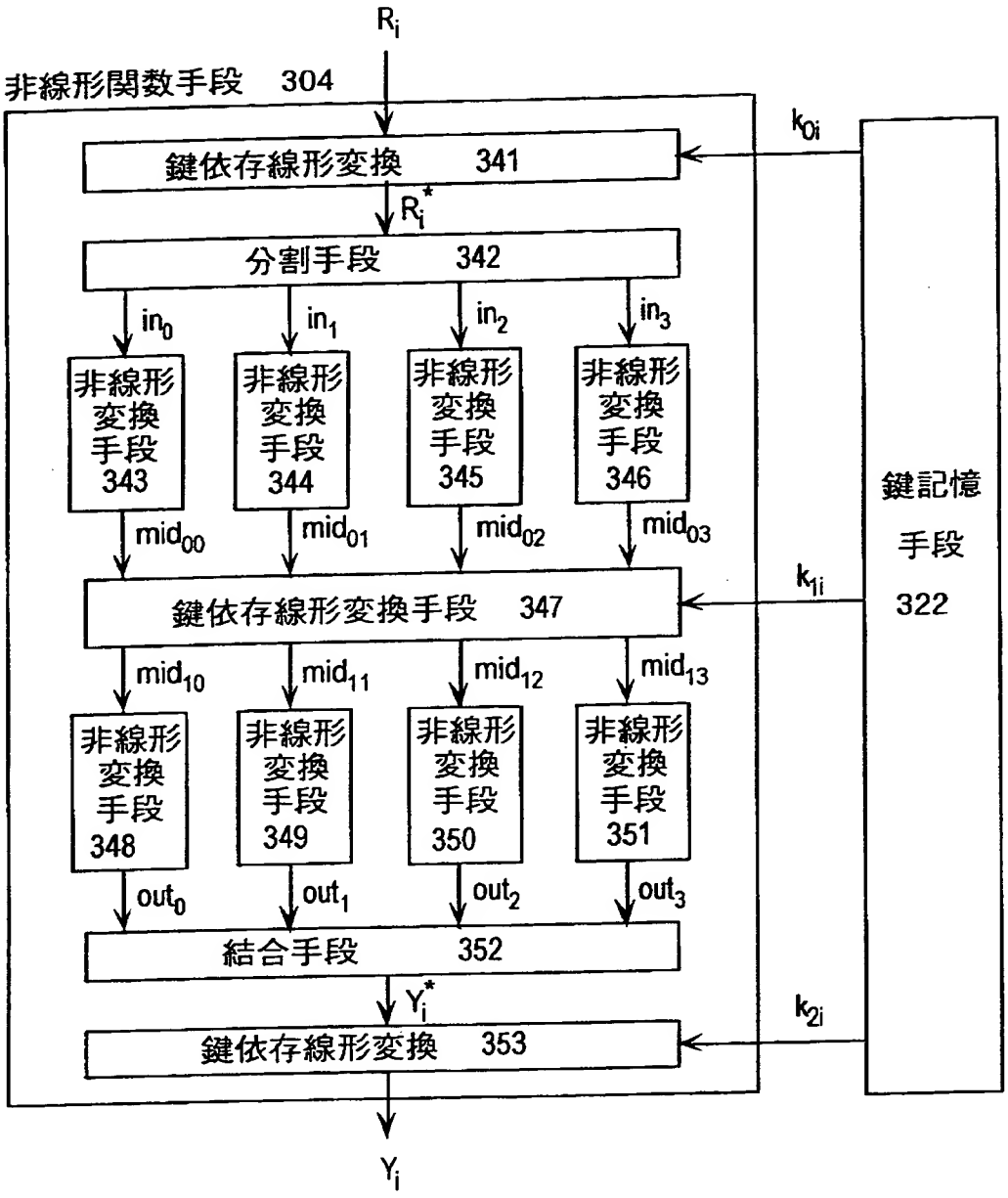
R_i
非線形関数手段　304
鍵依存線形変換　341
R_i^*
分割手段　342
in_0
in_1
in_2
in_3
非線形変換手段 343
非線形変換手段 344
非線形変換手段 345
非線形変換手段 346
mid_{00}
mid_{01}
mid_{02}
mid_{03}
鍵依存線形変換手段　347
mid_{10}
mid_{11}
mid_{12}
mid_{13}
非線形変換手段 348
非線形変換手段 349
非線形変換手段 350
非線形変換手段 351
out_0
out_1
out_2
out_3
結合手段　352
Y_i^*
鍵依存線形変換　353
Y_i
k_{0i}
k_{1i}
k_{2i}
鍵記憶手段 322

図 2

【図３】

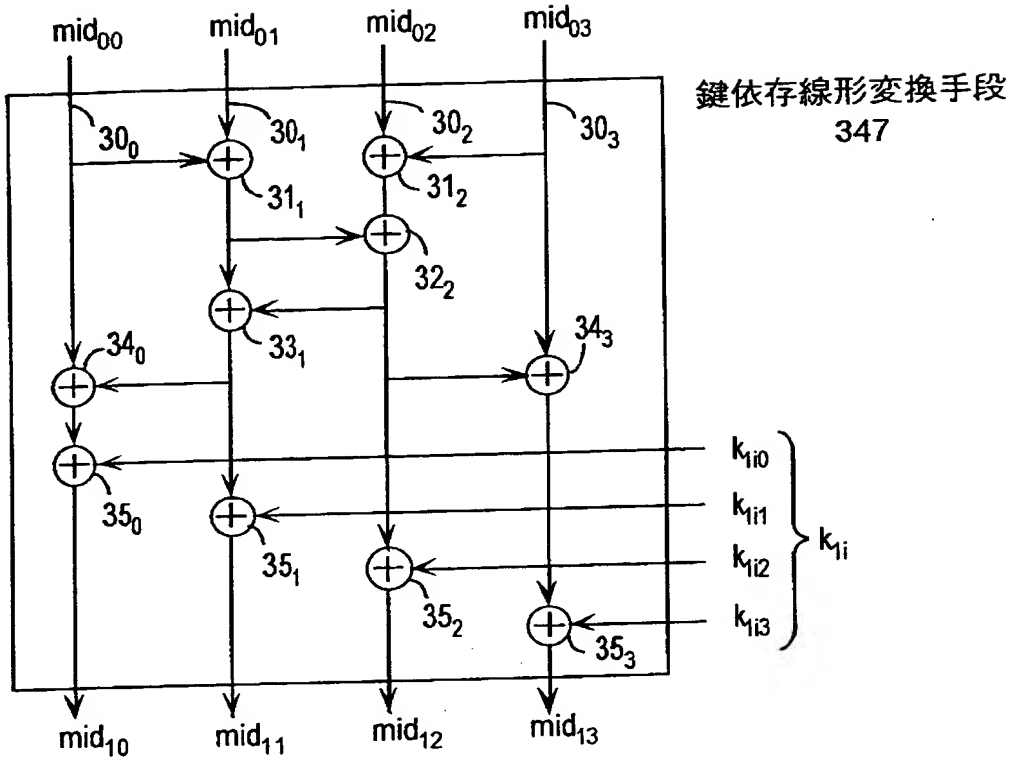
mid00
mid01
mid02
mid03
鍵依存線形変換手段
347
30₀
30₁
30₂
30₃
31₁
31₂
32₂
33₁
34₀
34₃
35₀
35₁
35₂
35₃
k1i0
k1i1
k1i2
k1i3
k1i
mid10
mid11
mid12
mid13

図3

【図４】

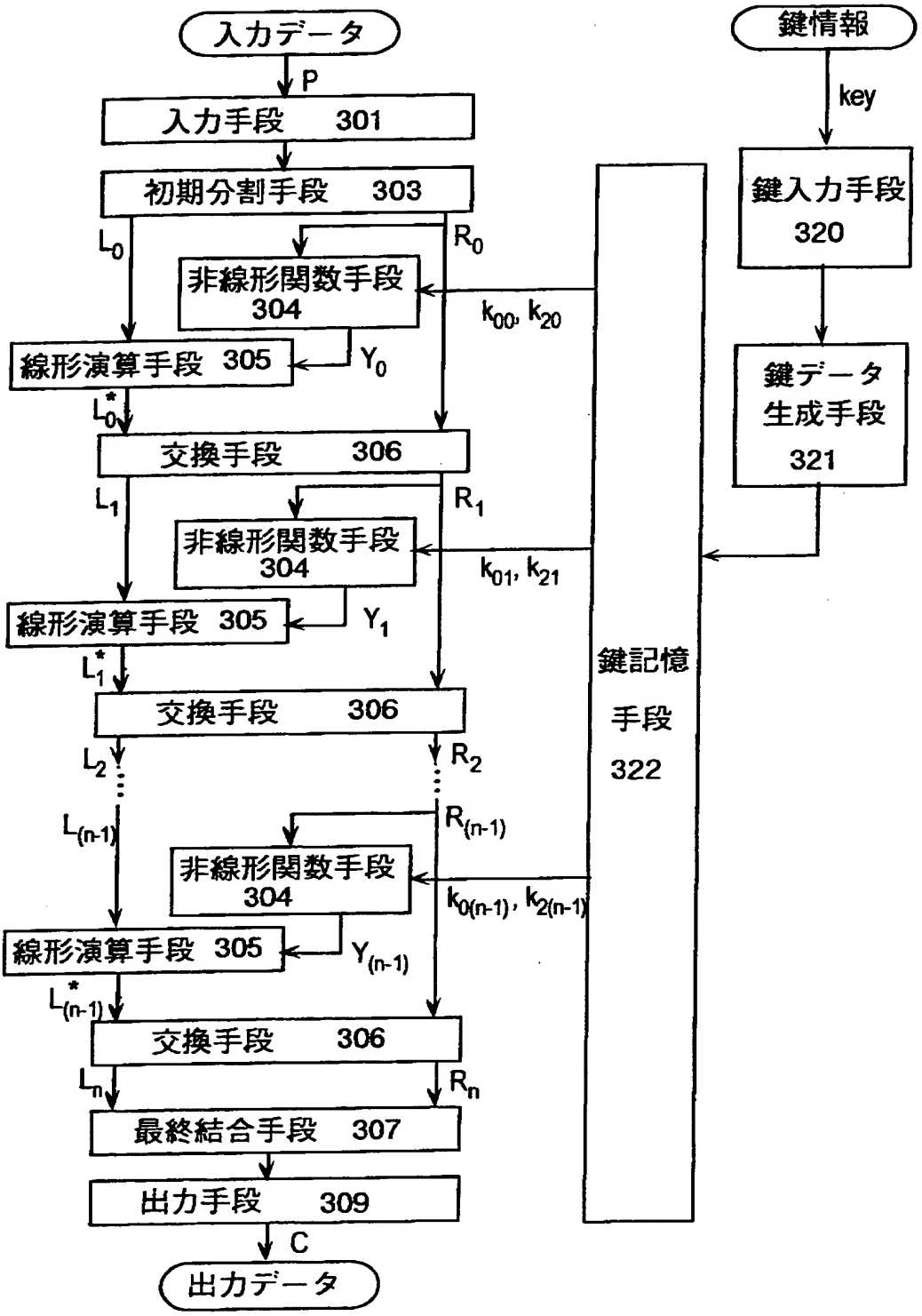
入力データ
P
入力手段　301
初期分割手段　303
L_0
R_0
非線形関数手段 304
k_{00}, k_{20}
線形演算手段 305
Y_0
L_0^*
交換手段　306
L_1
R_1
非線形関数手段 304
k_{01}, k_{21}
線形演算手段 305
Y_1
L_1^*
交換手段　306
L_2
R_2
$L_{(n-1)}$
$R_{(n-1)}$
非線形関数手段 304
$k_{0(n-1)}$, $k_{2(n-1)}$
線形演算手段 305
$Y_{(n-1)}$
$L_{(n-1)}^*$
交換手段　306
L_n
R_n
最終結合手段　307
出力手段　309
C
出力データ
鍵情報
key
鍵入力手段 320
鍵データ生成手段 321
鍵記憶手段 322

図 4

【図５】

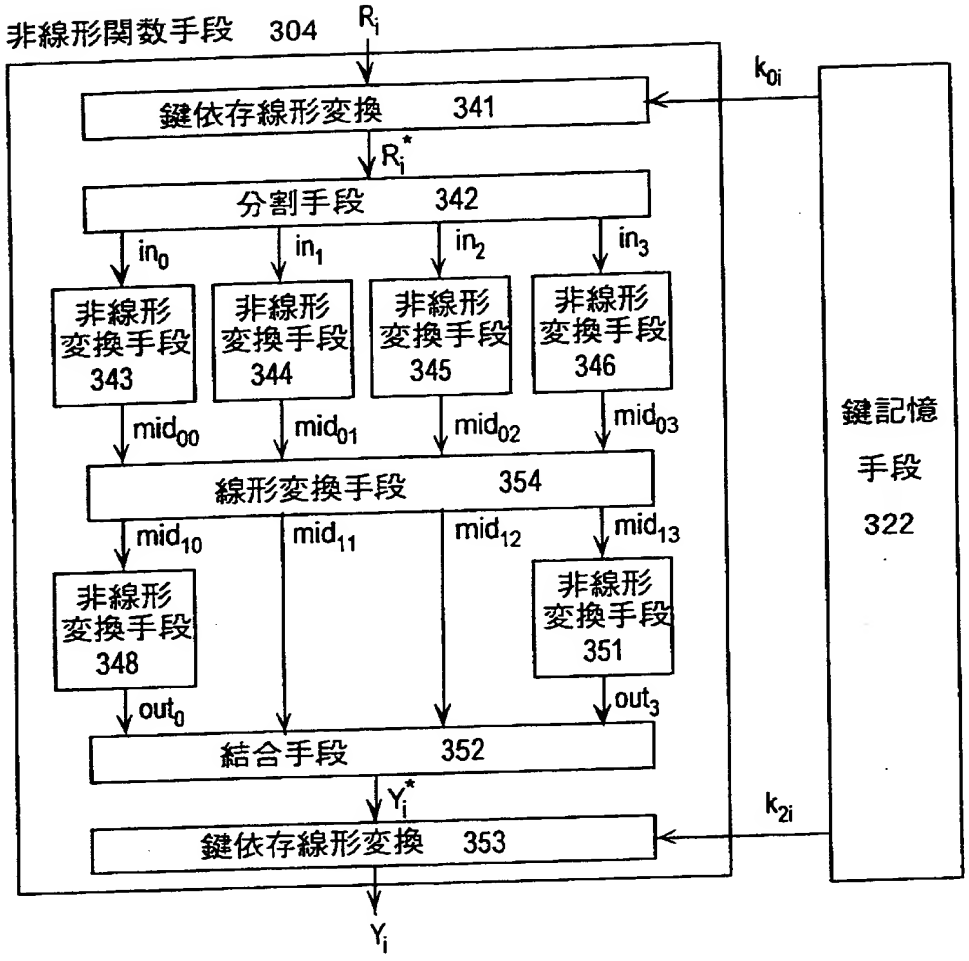
非線形関数手段　304
R_i
鍵依存線形変換　341
k_{0i}
R_i^*
分割手段　342
in_0
in_1
in_2
in_3
非線形変換手段 343
非線形変換手段 344
非線形変換手段 345
非線形変換手段 346
mid_{00}
mid_{01}
mid_{02}
mid_{03}
線形変換手段　354
mid_{10}
mid_{11}
mid_{12}
mid_{13}
非線形変換手段 348
非線形変換手段 351
out_0
out_3
結合手段　352
Y_i^*
k_{2i}
鍵依存線形変換　353
Y_i
鍵記憶手段 322

図５Ａ

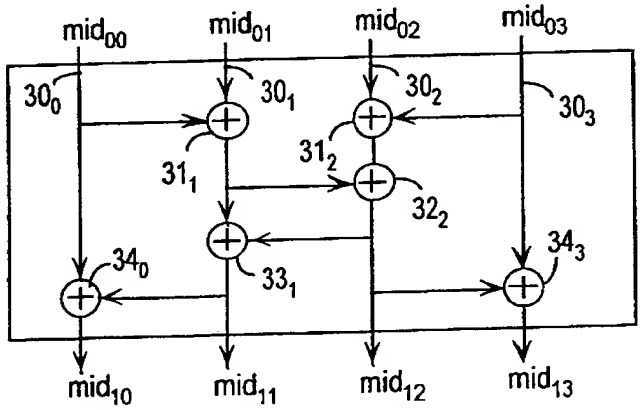
mid_{00}
mid_{01}
mid_{02}
mid_{03}
30_0
30_1
30_2
30_3
31_1
31_2
32_2
33_1
34_0
34_3
mid_{10}
mid_{11}
mid_{12}
mid_{13}
線形変換手段　354

図５Ｂ

【図６】

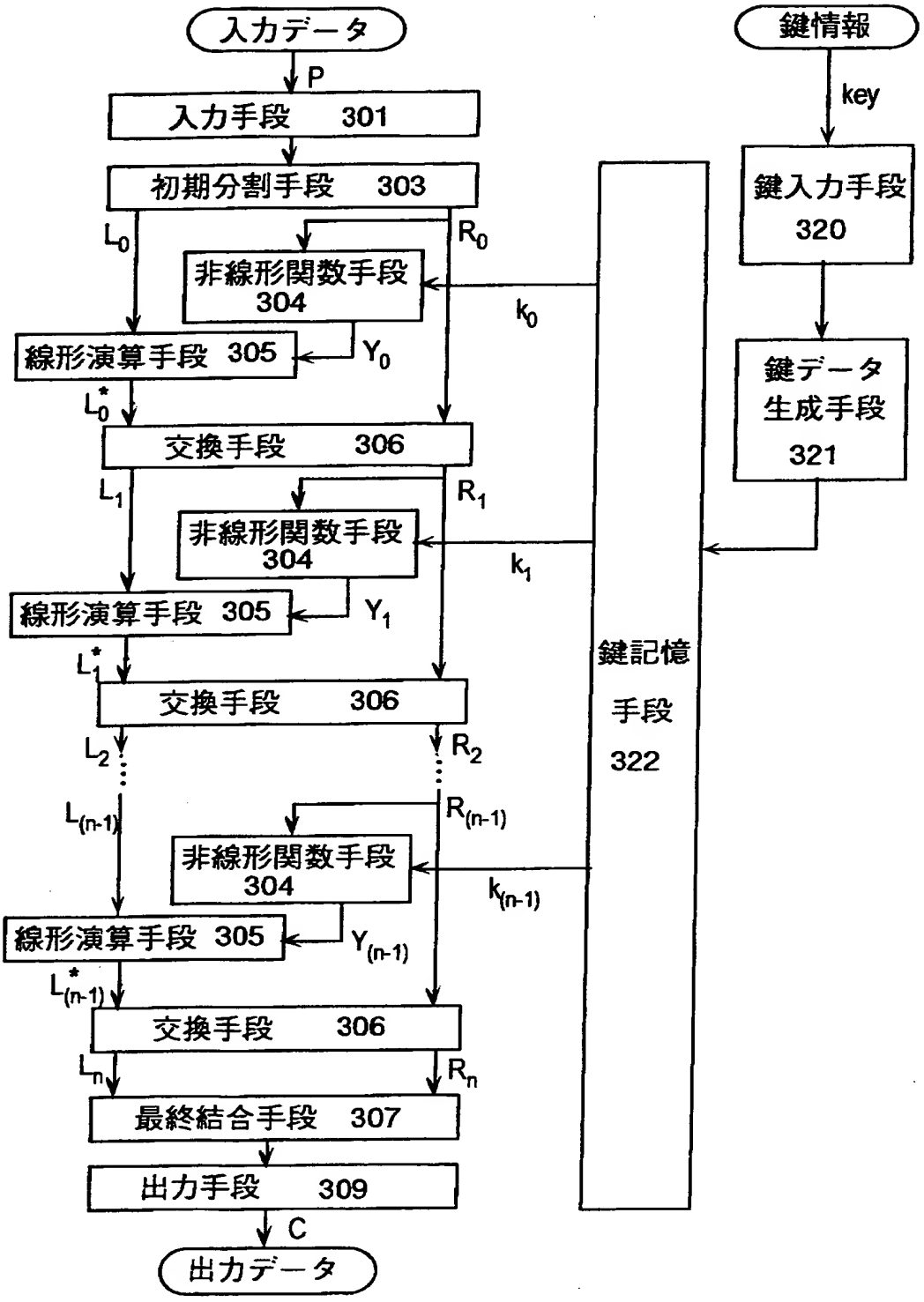
入力データ
P
入力手段　301
初期分割手段　303
L_0
R_0
非線形関数手段 304
k_0
線形演算手段 305
Y_0
L_0^*
交換手段　306
L_1
R_1
非線形関数手段 304
k_1
線形演算手段 305
Y_1
L_1^*
交換手段　306
L_2
R_2
$L_{(n-1)}$
$R_{(n-1)}$
非線形関数手段 304
$k_{(n-1)}$
線形演算手段 305
$Y_{(n-1)}$
$L_{(n-1)}^*$
交換手段　306
L_n
R_n
最終結合手段　307
出力手段　309
C
出力データ
鍵情報
key
鍵入力手段 320
鍵データ生成手段 321
鍵記憶手段 322

図６

【図7】

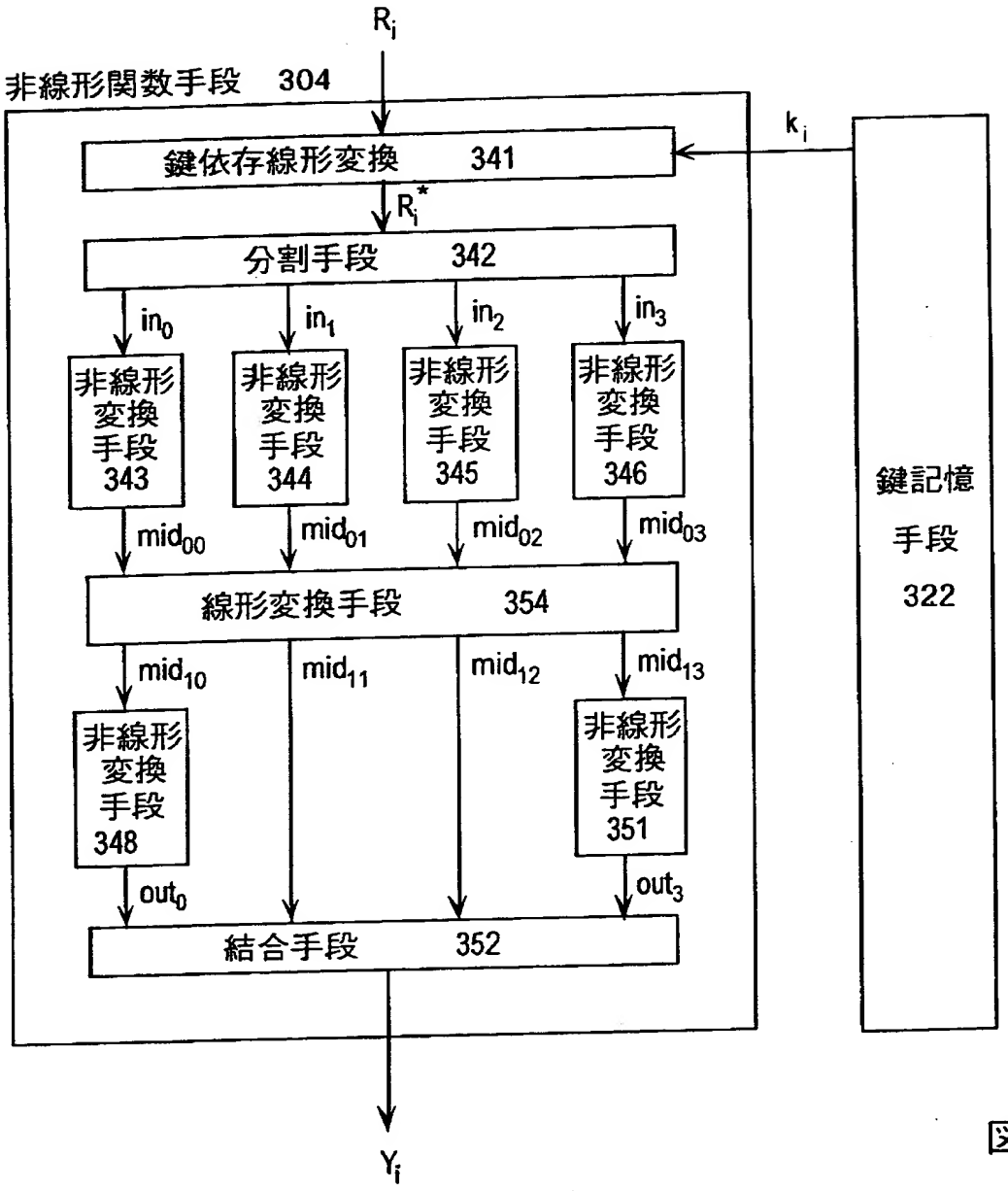
R_i
非線形関数手段　304
鍵依存線形変換　341
k_i
R_i*
分割手段　342
in_0
in_1
in_2
in_3
非線形変換手段 343
非線形変換手段 344
非線形変換手段 345
非線形変換手段 346
mid_00
mid_01
mid_02
mid_03
線形変換手段　354
mid_10
mid_11
mid_12
mid_13
非線形変換手段 348
非線形変換手段 351
out_0
out_3
結合手段　352
Y_i
鍵記憶手段 322

図7

【図８】

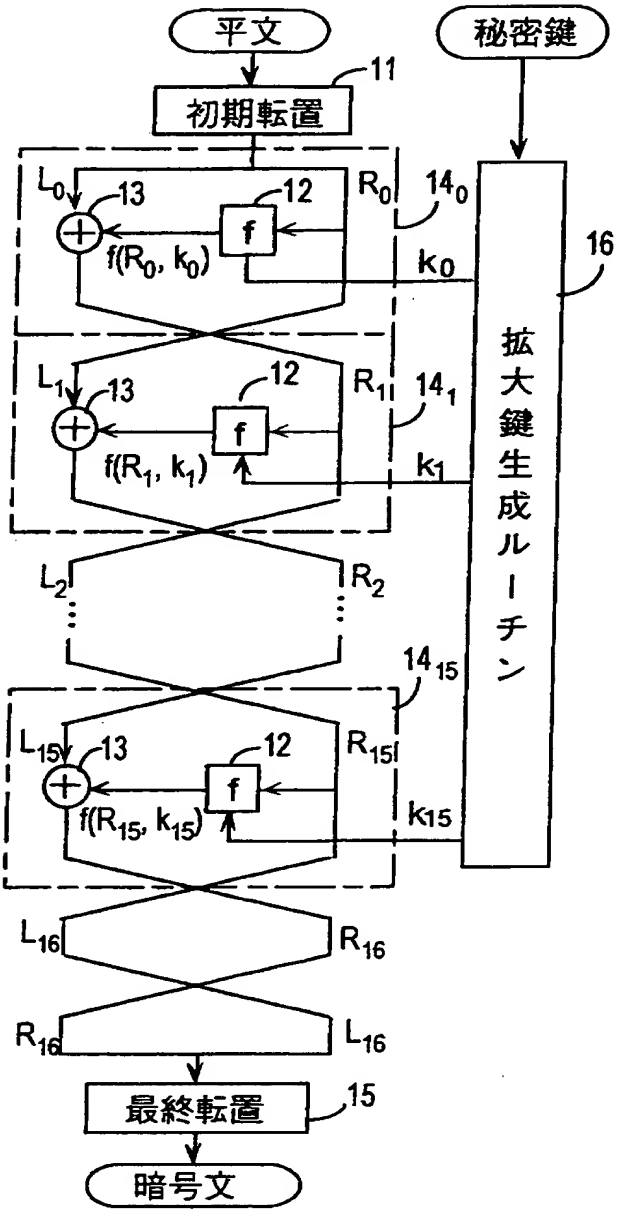
平文
秘密鍵
11
初期転置
L_0
13
12
R_0
14_0
f
$f(R_0, k_0)$
k_0
16
L_1
13
12
R_1
14_1
f
$f(R_1, k_1)$
k_1
拡大鍵生成ルーチン
L_2
R_2
14_{15}
L_{15}
13
12
R_{15}
f
$f(R_{15}, k_{15})$
k_{15}
L_{16}
R_{16}
R_{16}
L_{16}
最終転置
15
暗号文

図８

【図９】

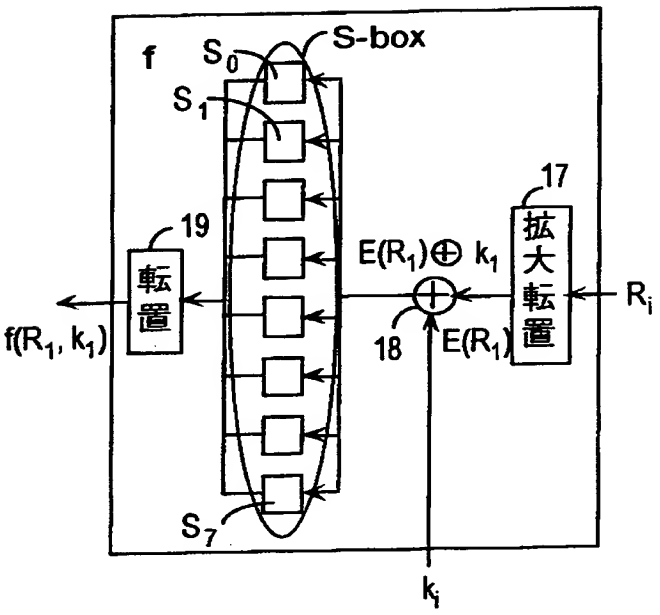

図９

【書類名】　　要約書

【要約】

【課題】　差分解読法、線形解読法に対して安全性が高く、かつ高速処理が可能。

【解決手段】　入力データをL_0，R_0に分割し、Rを非線形関数手段３０４で鍵に応じて交換し、その出力と、もとの排他的論理和をとった出力をR_1とし、R_0をL_1とすることを複数回行い、手段３０４として、入力R_iを鍵依存線形変換し（３４１）、その出力をin_0，in_1，in_2，in_3に４分割し、これらをそれぞれ非線形変換し（３４３～３４６）、これら変換出力を鍵依存線形変換手段３４７で相互に関連づけると共に鍵k_{i0}～k_{i03}を排他的論理和をとり、その各出力をそれぞれ非線形変換し（３４８～３５１）、その変換出力をビット結合し、更にk_{2i}で鍵依存線形変換して出力とする。

【選択図】　　図２

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000004226
【住所又は居所】　東京都新宿区西新宿三丁目１９番２号
【氏名又は名称】　日本電信電話株式会社
【特許出願人】
【識別番号】　591230295
【住所又は居所】　東京都渋谷区桜丘町２０番１号
【氏名又は名称】　エヌティティエレクトロニクス株式会社
【代理人】　申請人
【識別番号】　100066153
【住所又は居所】　東京都新宿区新宿四丁目２番２１号　相模ビル
【氏名又は名称】　草野　卓

出　願　人　履　歴　情　報

識別番号　　〔000004226〕

1．変更年月日　　1995年　9月21日
　〔変更理由〕　　住所変更
　　住　所　　東京都新宿区西新宿三丁目19番2号
　　氏　名　　日本電信電話株式会社

出　願　人　履　歴　情　報

識別番号　　〔591230295〕

1．変更年月日　　1991年　9月19日
　[変更理由]　新規登録
　　住　所　東京都武蔵野市吉祥寺本町1丁目14番5号
　　氏　名　エヌティティエレクトロニクステクノロジー株式会社

2．変更年月日　　1997年　7月24日
　[変更理由]　名称変更
　　住　所　東京都渋谷区桜丘町20番1号
　　氏　名　エヌティティエレクトロニクス株式会社